Capita | entrust Inspiring Futures

Filtering and monitoring – essential information for Designated Safeguarding Leads

Vikki Bott

October 2023

Aims of the session

Understand and work to meet your statutory requirements in relation to filtering and monitoring

Know and understand the expectations included in the filtering and monitoring standards from the DfE and how it affects you in your role and your organisation as a whole

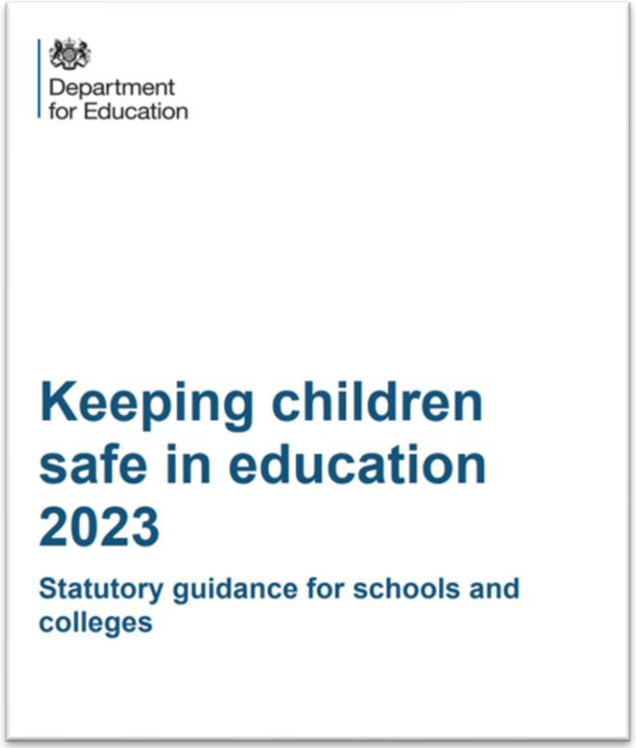
Understand and develop your organisations safeguarding rationale for the filtering approach implemented in your organisation

Understand and develop your organisations approach to monitoring that meets the needs of all users

Have resources and information that will support you to undertake a review of filtering and monitoring systems against the expectations included in the DfE filtering and monitoring standards for schools and colleges

Statutory guidance and standards

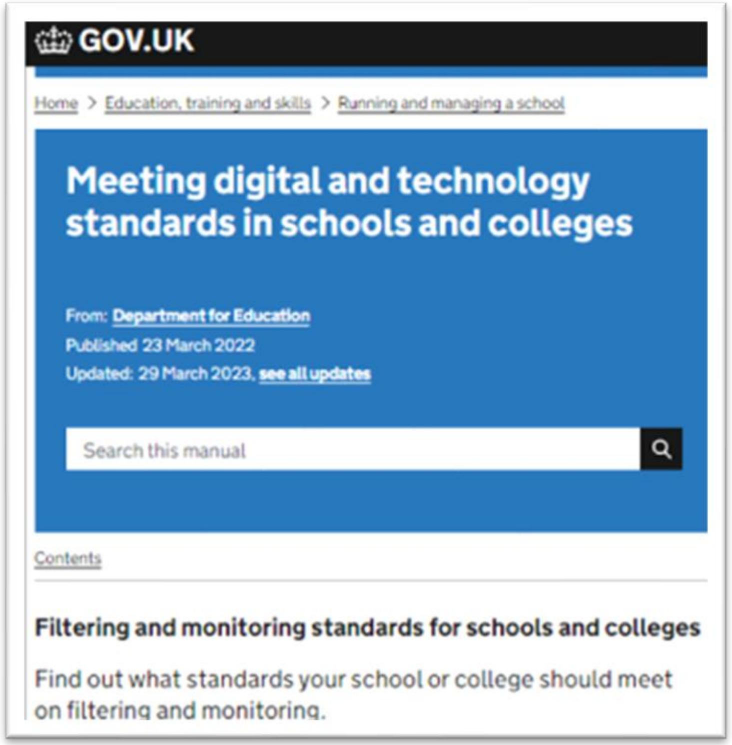
Statutory guidance and standards



Department for Education

Keeping children safe in education 2023

Statutory guidance for schools and colleges



GOV.UK

Home > Education, training and skills > Running and managing a school

Meeting digital and technology standards in schools and colleges

From: Department for Education

Published 23 March 2022

Updated: 29 March 2023, see all updates

Search this manual

Contents

Filtering and monitoring standards for schools and colleges

Find out what standards your school or college should meet on filtering and monitoring.

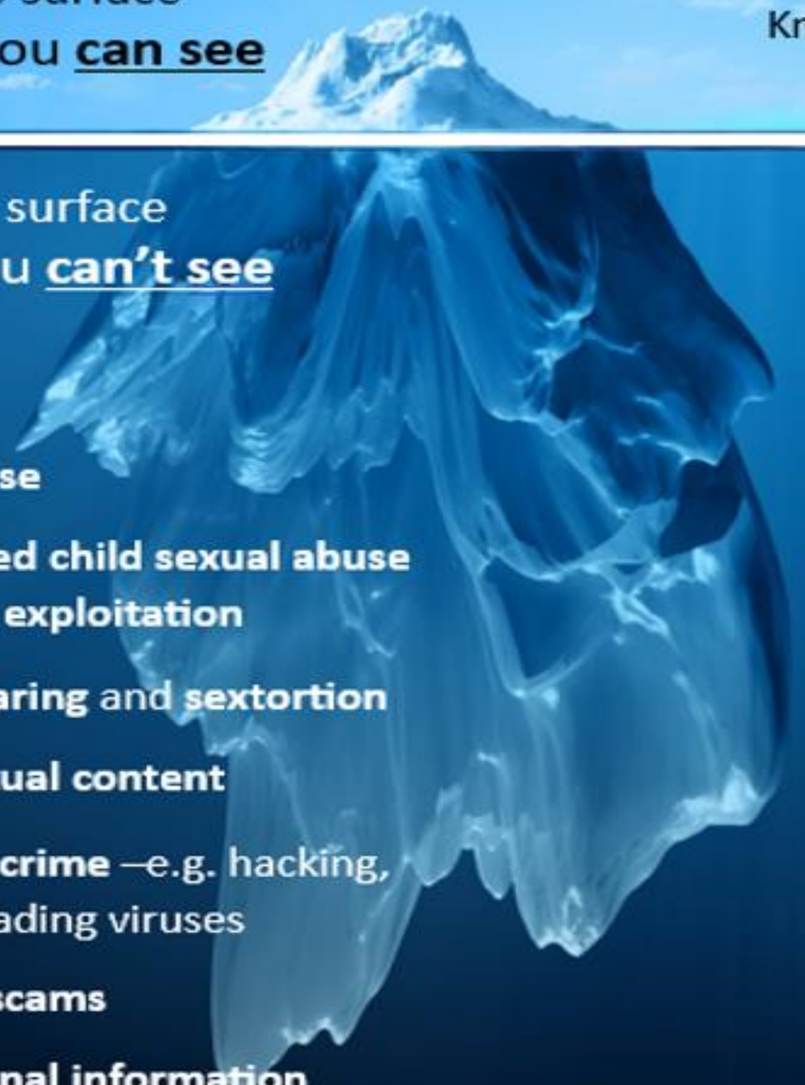
Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Why must schools act on new filtering and monitoring standards?

Children’s Commissioner urges action to prevent another tragedy.

The Coroner’s inquest, which concluded in 2021, found that Frankie had accessed dangerous content containing descriptions of suicide and self-harm on a school laptop and iPad during school hours. The Coroner concluded that both the content which Frankie viewed, and failures by the school to protect her from it, directly contributed to Frankie’s decision to take her own life.

Both the failures of the tech platform on which Frankie accessed graphic self-harm and suicide content, and the school’s defective filtering and monitoring tools were hopeless.



Above the surface
Offline risks you **can see**

Changes in **behaviour**

Deterioration in **academic performance**

Injuries/bruises

Absenteeism

Known **domestic risk**

Requests for **help**

Below the surface
Online risks you **can't see**

Child-on-child **abuse**

Technology-assisted child sexual abuse and **child criminal exploitation**

Harmful **image sharing** and **sextortion**

Self-generated **sexual content**

Cyber-dependent crime –e.g. hacking, creating, and spreading viruses

Online fraud and **scams**

Oversharing **personal information**

Online conversations/social media/gaming chat about drugs/extremism, being harmed/intention to harm, and/or with inappropriate adults

Tech abuse linked to domestic abuse and teenage relationship abuse

Membership of online groups - Incels

Bullying/violence towards others or received

Searches for **risk-based content** – suicide, self-harm

Inappropriate content accessed via streaming or social media – challenges or violence

Feelings and emotions typed in a document

Time spent engaging in the same activity

What are your statutory obligations for filtering and monitoring?

*103. …The **designated safeguarding lead** should take **lead responsibility** for safeguarding and child protection (including online safety and **understanding the filtering and monitoring systems and processes in place**). This should be explicit in the role holder's job description.*

*14. **All staff** should receive appropriate **safeguarding and child protection training (including online safety** which, amongst other things, includes an **understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction**.*

What are your statutory obligations for filtering and monitoring?

*124. **Governing bodies** and proprietors should **ensure that all staff undergo safeguarding and child protection training (including online safety** which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction.*

*134. Whilst it is essential that **governing bodies** and proprietors ensure that appropriate filtering and monitoring systems are in place, they **should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding**.*

What are your statutory obligations for filtering and monitoring?

138. Online safety and the school or college's approach to it should be ***reflected in the child protection policy*** *which, amongst other things, should* ***include appropriate filtering and monitoring on school devices and school networks****.*

141. …governing bodies and proprietors should be doing all that they reasonably can to ***limit children's exposure to the four risks*** *from the school's or college's IT system….governing bodies and proprietors should ensure their school or college has* ***appropriate filtering and monitoring systems in place and regularly review their effectiveness… leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns*** *when identified. Governing bodies and proprietors should consider the* ***number of*** *and* ***age range of their children, those who are potentially at greater risk of harm*** *and* ***how often they access the IT system*** *along with the* ***proportionality of costs versus safeguarding risks***

What are your statutory obligations for filtering and monitoring?

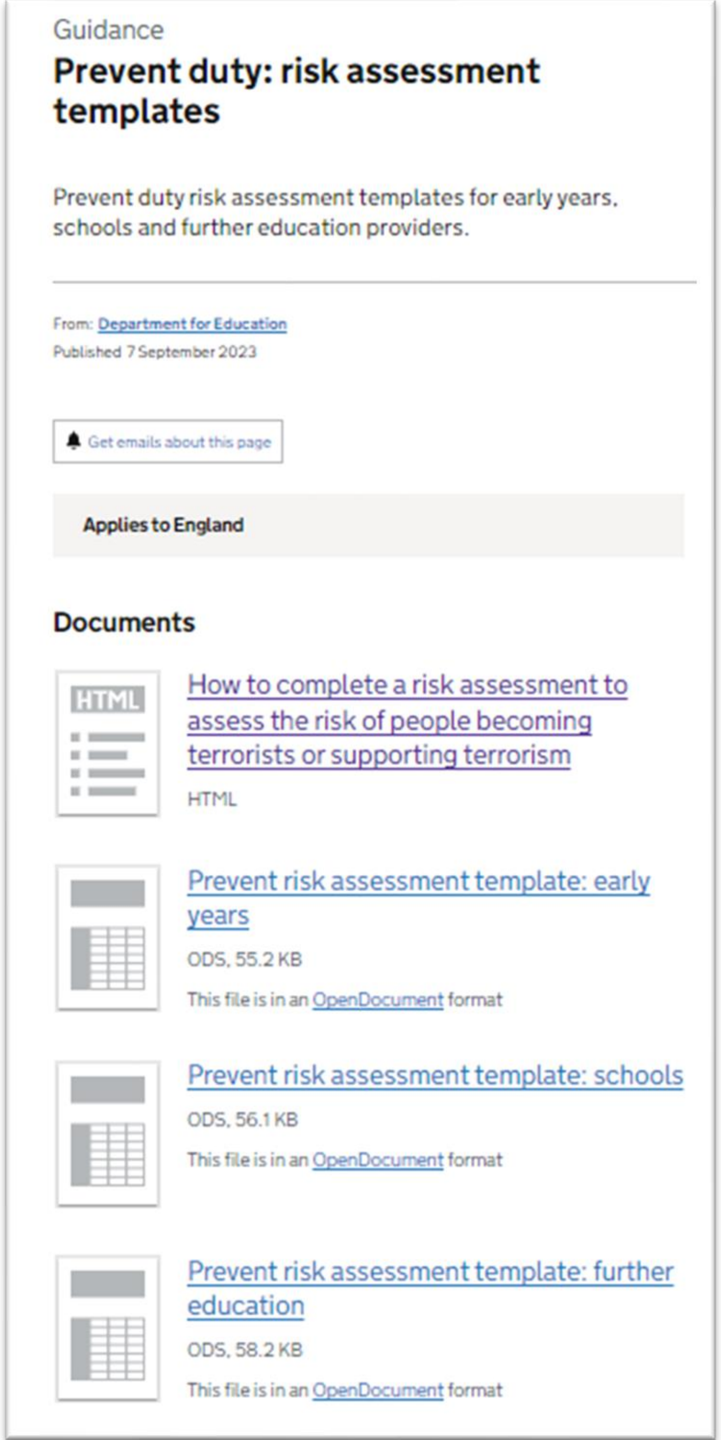
*142. The **appropriateness of any filtering and monitoring systems** are a matter for individual schools and colleges and will be **informed in part, by the risk assessment required by the Prevent Duty.***

*Annex A: **All staff should receive appropriate safeguarding and child protection training (including online safety** which, amongst other things, includes an understanding of the expectations, **applicable roles and responsibilities in relation to filtering and monitoring**) which is regularly updated. In addition, all staff should receive safeguarding and child protection updates (including online safety) (for example, via emails, e-bulletins and staff meetings), as required, and at least annually, to provide them with the skills and knowledge to safeguard children effectively*

Prevent duty update in effect from 31st December 2023

HM Government

Prevent duty guidance:
Guidance for specified authorities in England and Wales



Guidance

Prevent duty: risk assessment templates

Prevent duty risk assessment templates for early years, schools and further education providers.

From: Department for Education
Published 7 September 2023

Get emails about this page

Applies to England

Documents

How to complete a risk assessment to assess the risk of people becoming terrorists or supporting terrorism
HTML

Prevent risk assessment template: early years
ODS, 55.2 KB
This file is in an OpenDocument format

Prevent risk assessment template: schools
ODS, 56.1 KB
This file is in an OpenDocument format

Prevent risk assessment template: further education
ODS, 58.2 KB
This file is in an OpenDocument format

https://www.gov.uk/government/publications/prevent-duty-risk-assessment-templates

Updated Prevent in effect from 31st December 2023

IT policies

186. Settings will likely already have **policies** relating to the **appropriate use of their IT equipment and networks**, which should **contain specific reference to the Prevent duty**. Many settings already **use filtering** as a means of **restricting access to harmful content** and should **consider the use of filters as part of their overall strategy to prevent people from becoming involved in, or supporting, terrorism**.

187. The **content and proportionality of these policies** are a matter for providers and **will be informed, in part, by the Prevent risk assessment**.

188. For **further and higher education** providers, there should be **clear policies in place for students and staff using IT equipment and networks to research terrorism and counter-terrorism in the course of their learning**.

Prevent duty risk assessment template

Category	Risk	Hazard	Risk management	RAG	Further action needed
IT policies	Ineffective IT policies increases the likelihood of students & staff being drawn into extremist material and narrative online. Inappropriate internet use by students is not identified or followed up.	Students can access terrorist & extremist material when accessing the internet at the institution.	[Example] Settings should ensure appropriate internet filtering is in place.		
		Students may distribute extremist material using the institutions IT system.	[Example] Settings should ensure that there is a clear reporting process in place should filtering systems flag any safeguarding or Prevent-related concerns.		
		Unclear linkages between IT policy and the Prevent duty. No consideration of filtering as a means of restricting access to harmful content.	[Example] The DSL should take lead responsibility for safeguarding and child protection (including online safety)		
			[Example] Settings should equip children and YP with the skills to stay safe online, both in school and outside.		

The Prevent Duty

1. Is your filtering provider signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?

2. Is your filtering system operational, up to date and applied to all:

- users, including guest accounts?
- school owned devices?
- devices using the school broadband connection?

3. Does your filtering system allow you to identify:

- device name or ID, IP address, and where possible, the individual?
- the time and date of attempted access?
- the search term or content being blocked?

In addition…

*70. It is important for children to **receive the right help** at the **right time** to **address safeguarding risks, prevent issues escalating and to promote children's welfare**.*

*450. HSB…**Addressing inappropriate behaviour** can be an **important intervention** that helps **prevent problematic, abusive and/or violent behaviour in the future**.*

*491. …. Early help means **providing support as soon as a problem emerges**, at any point in a child's life. Providing early help is **more effective in promoting the welfare of children than reacting later**.*

*543. …. It is important that the **perpetrator(s)** is/are also **given the correct support** to try to **stop them re-offending** and to **address any underlying** trauma that may be causing this behaviour.*

*Annex B. …Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into **cyber-dependent crime**.*
*If there are concerns about a child in this area, the designated safeguarding lead (or deputy), should consider **referring into the Cyber Choices programme**.*

Ofsted monitoring of safeguarding, may ask:

How safe do your pupils feel in school when using devices?

How does your school protect children with special educational needs from the dangers online?

How does your school effectively protect vulnerable children from accessing harmful content?

How is social media tackled within your school?

How does your school ensure students can access the internet in an age-appropriate way?

How does the school identify whether policies are clear, understood and adhered to?

What monitoring solution does the school have in place to support pupils and staff with online safety?

Does your monitoring solution protect pupils from accessing radicalisation & extremist content?

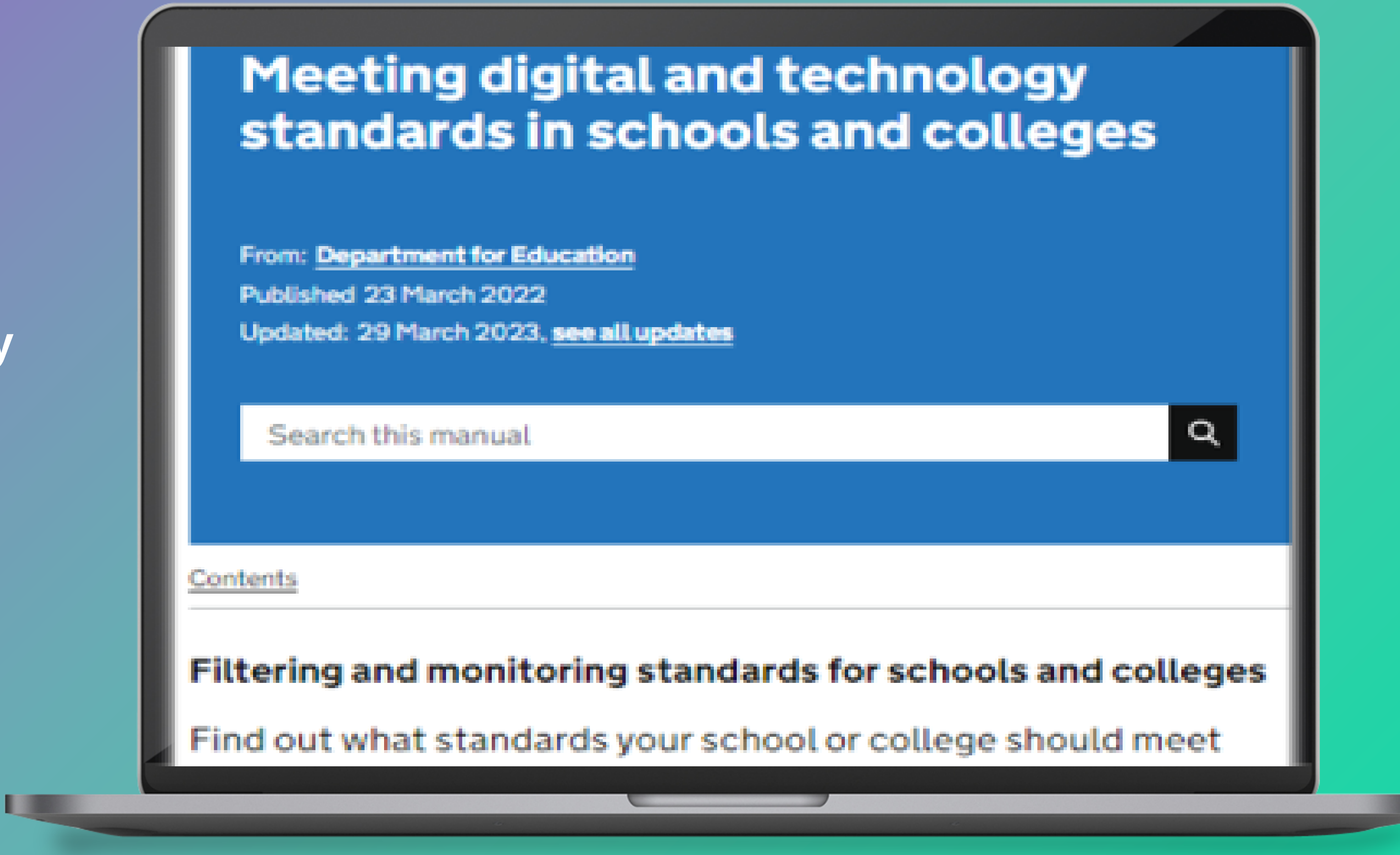
How are incidents dealt with and recorded?

Do your governors understand how the monitoring solution is used within the school?

DfE Meeting digital and technology standards in schools and colleges

Filtering and monitoring standards in schools and colleges

1. You should **identify** and **assign roles and responsibilities** to **manage your filtering and monitoring systems**
2. You should **review your filtering and monitoring provision** at **least annually**
3. Your **filtering system** should **block harmful and inappropriate content, without unreasonably impacting teaching and learning**
4. You should have **effective monitoring strategies** that **meet the safeguarding needs of your school or college**



Meeting digital and technology standards in schools and colleges

From: Department for Education

Published 23 March 2022

Updated: 29 March 2023, see all updates

Filtering and monitoring standards for schools and colleges

Find out what standards your school or college should meet

What is filtering and monitoring and how do they work?

Filtering

Software that restricts or controls the content an Internet user is able to access. Internet filters can be installed by anyone who maintains a network.

Managed filtering can work on a user group basis allowing different restrictions depending on the group you are allocated to.

Categories of content should be blocked in schools*.

Sites can be added to a blocklist which will be blocked or an allowlist to be allowed. Sites that are blocked can be unblocked if required.

Find out:

Do you have **safe search** enforced?

Is **safe search** enforced on the **network**, **devices** or **both**?

What **search engine(s)** is **safe search** enforced on? Do you block other search engines that don’t have it enforced?

Do you have **SSL inspection** enabled?

The setting needs to be enabled AND a certificate needs to be installed on each device.

Categories that should be blocked in school

IWF Child Sexual Abuse Material – **illegal content**

Home Office police assessed list of unlawful terrorist content – **illegal content**

Inappropriate content:

Discrimination – Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010

Drugs / Substance abuse – displays or promotes the illegal use of drugs or substances

Extremism – promotes terrorism and terrorist ideologies, violence or intolerance

Gambling – enables gambling

Malware / Hacking – promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content

Pornography – displays sexual acts or explicit images

Piracy and copyright theft – includes illegal provision of copyrighted material

Self-Harm – promotes or displays deliberate self-harm (including suicide and eating disorders)

Violence – displays or promotes the use of physical force intended to hurt or kill

Find out…

- Who is your filtering provider?
- What filtering product do they provide?
- Is the filtering product a managed filtering solution?
- Can you set different filtering policies for specific users and user groups?
- How can temporary or permanent changes be made and who by?
- Do they block access to illegal content?
- Can you add your own keywords to the filter library that represent new concerns in your organisation?
- Does filtering work if devices are taken home?
- What traffic logs and analytics are provided?
- Does it provide any real-time alerts when a user’s behaviour may be cause for concern?

Broadband providers and filtering products include:

Broadband provider - **Exa** with filtering product - **Surfprotect**

Broadband provider - **Updata** with filtering product - **Netsweeper**

Broadband provider - **CityFibre** with filtering product - **Smoothwall**

Other filtering providers include:

Lightspeed

Senso

Sophos

RM Education

Fortinet

Monitoring

Physical

Internet and web access

Active technology monitoring services

Pro-active technology monitoring services

Securus Monitoring is Entrust’s **active technology monitoring** product for schools that is **self-managed**

Digital Monitoring Service is Entrust’s **proactive technology monitoring** service for schools that is a **managed monitoring service**

Active technology monitoring applications may include:

- Monitoring any device that connects to the school network
- Monitoring personal devices for BYOD
- Keyboard and/or screen captures
- Online and offline activity
- Library monitoring topics of concern, may include the ability to configure library
- Detailed screenshot evidence highlighting capture words and phrases in real time, may also include defined severity ratings
- Monitor popular applications and internet browsers on the school network
- Dashboard and reporting platform, may include the ability to configure and customise reports and include email alert functionality to follow students at particular risk
- Integration with other safeguarding reporting tools e.g. CPOMS and MYCONCERN
- Multi-language compatibility and local language, acronyms and algospeak
- Active Directory synchronisation

All staff need to know that:

Technical monitoring systems **do not stop unsafe activities** on a device or online. Therefore, staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

DO NOT rely alone on the technical monitoring system to take away all of your concerns of not knowing when users are engaging in unsafe activities!

Examples of libraries of concern

- Cyber bullying
- Suicide and self-harm
- Mental health issues
- Racism and discrimination

- Hacking
- Gang culture
- Substance abuse
- Sexual abuse and grooming

Entrust’s Monitoring Service – Top 5 categories captured

Pornography 20%

Suicide risk 16% (12% for 2022)

Sexual behaviour 15%

Emotional health 10% (6% for 2022)

Bullying 8%

27 incidents related to Cyber security which has increased over the last two years

Examples of grading systems and actions:

Grade 1 - False positive, no action required

Grade 2 - Off task e.g., playing games. If this appears to be excessive or obsessive, Entrust's managed monitoring will e-mail the school contacts

Grade 3 - Behaviour, inappropriate language or one-off incidents. If using Entrust's managed monitoring AND a primary school, then an e-mail is sent to the named contacts

Grade 4 - Potential safeguarding issue with no immediate risk of harm. If using Entrust's managed monitoring, then an e-mail is sent to the named contacts

Grade 5 - Potential safeguarding issue with immediate risk of harm. If using Entrust's managed monitoring, then a telephone call and e-mail to the named contacts

Entrust’s Monitoring Service – Grade 4 and 5 captures

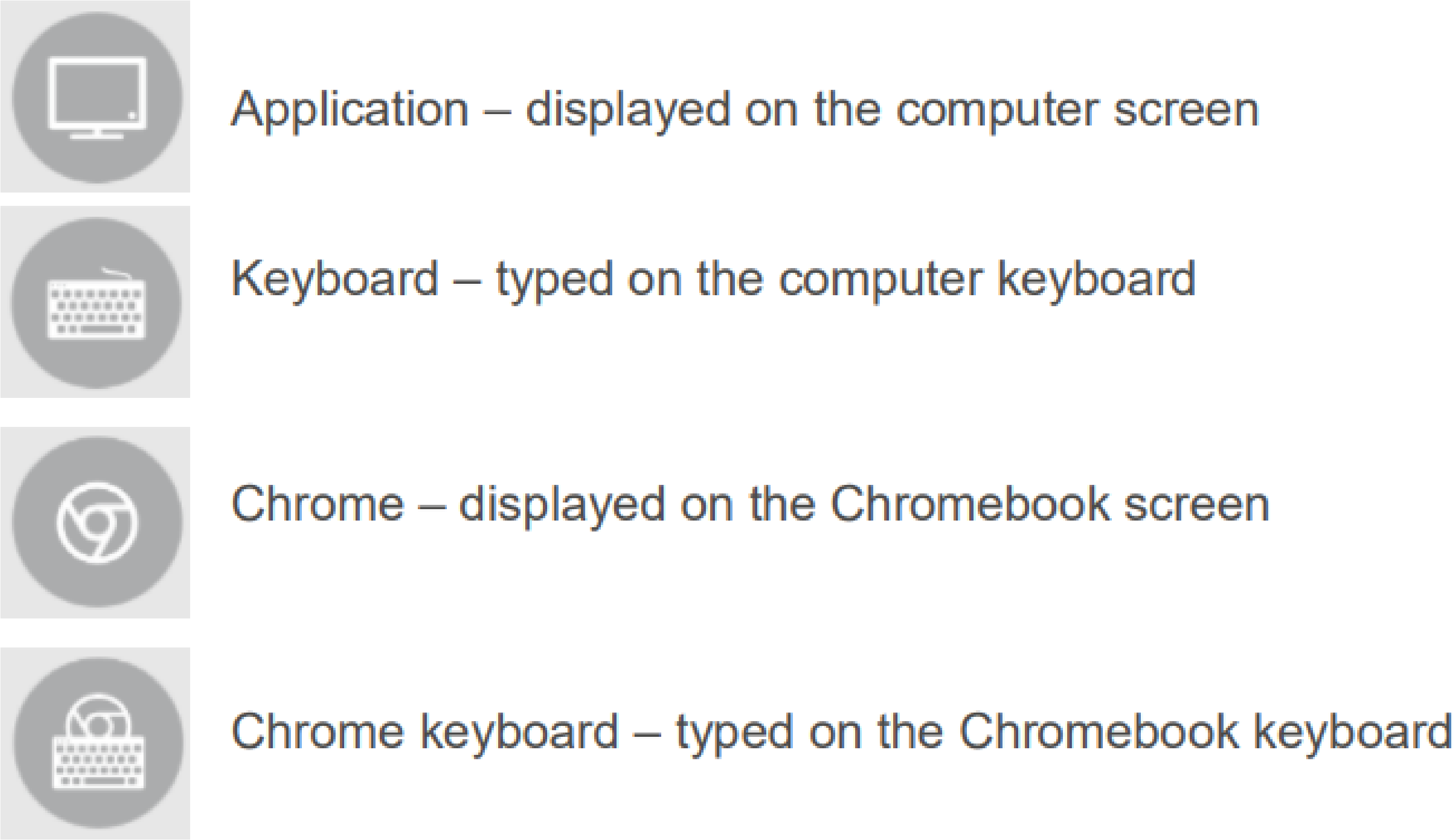
Organisation type	Grade 4	Grade 5
Primary	89	11
Secondary	789	136
Special	26	3

What activity can be captured?

Keyboard captures – as the child types, if what they type triggers a violation against the library a screen shot of their screen will be taken and reported through the dashboard

Desktop/screen/application captures – any incoming communication and non-typed content is being monitored against the library and if a violation occurs a screen shot is taken and reported through the dashboard

Securus source captures include:



Application – displayed on the computer screen

Keyboard – typed on the computer keyboard

Chrome – displayed on the Chromebook screen

Chrome keyboard – typed on the Chromebook keyboard

Active technology monitoring providers include

Securus
Safeguard Monitor Protect

smoothwall®

NetSupport

Impero

senso.
Classroom Management Software

securly

Lightspeed Systems®

Mobile devices may work differently to other devices for monitoring

iPad monitoring is limited due to Apples data privacy features.

Internet activity through a browser on iPad can be monitored

iPad doesn’t always require a log in making identifying a user difficult.

Securus Net can authenticate a user on an iPad through things such as LDAP (windows credentials), Google, Azure details.

Mobile devices and active technical monitoring systems

- Know what mobile devices you have
- What apps do they use?
- How are the mobile devices managed?
- Are they locked down as managed devices so software cannot be un/installed except by school administrators?
- Carry out tests on your filtering and monitoring solution to check they are working across all mobile devices, across installed apps (not just internet browsers)
- Identify any vulnerable users of mobile devices, paying particular attention to ensure harmful content is not accessible on specific devices

Active technology monitoring applications and filtering systems do not

Monitor personal devices that have access to their own data for example, 3G, 4G and 5G connections.

The use of personal devices with own data plans must be carefully managed through policies and guidelines for use with acceptable user agreements.

DfE Meeting digital and technology standards in schools and colleges

Filtering and monitoring standards in schools and colleges

1. Roles and responsibilities

Filtering and monitoring

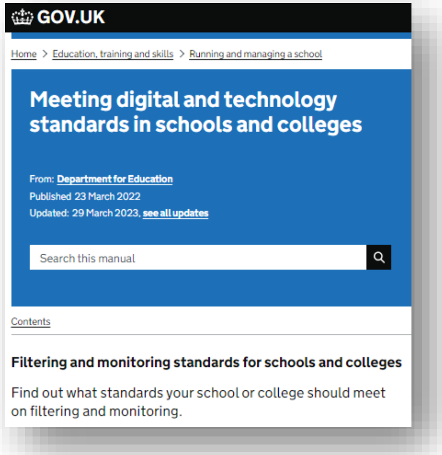
*103. …*The **designated safeguarding lead** should take **lead responsibility** for safeguarding and child protection (including online safety and **understanding the filtering and monitoring systems and processes in place**). This should be explicit in the role holder's job description.

Have you undertaken a review of filtering system requirements and monitoring strategies, drawing on policy documents, the risk profile of learners and the expectations included in relevant standards?

What is your rationale for the filtering approach implemented in your school?

Are you confident that your monitoring strategy meets the needs of all school users?

1. Roles and responsibilities to manage filtering and monitoring systems



Home > Education, training and skills > Running and managing a school

Meeting digital and technology standards in schools and colleges

From: Department for Education
Published 23 March 2022
Updated: 29 March 2023, see all updates

Filtering and monitoring standards for schools and colleges

Find out what standards your school or college should meet on filtering and monitoring.

DSL responsibility could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

Other roles and responsibilities to consider

SLT role:

- Making sure standards are met
- Procurement of systems
- Staff training, knowledge and skills to improve confidence and empower them
- Policies and procedures
- Reviewing effectiveness of systems and processes
- Documenting decisions – what is blocked and why
- Responding to incident reports

Safeguarding governor:

- Strategic responsibility
- Need assurance systems and processes are working to protect users
- Meet regularly with the DSL and SLT to review systems
- Establish roles and responsibilities of staff
- Ensure timely changes are implemented

Other roles and responsibilities to consider

- Be clear who is monitoring what:

  the DSL and deputies monitor pupil logs and reports

  it should be a member of SLT that monitors staff logs and reports

- All teachers should be fully aware of how filtering and monitoring systems used by your organisation work

Responding to incidents out of hours

What will you respond to and when will the alerts be checked and responded to outside of working hours?

Have governors considered 24/7 monitoring? Whilst it is essential that governing bodies ensure that appropriate filtering and monitoring systems are in place, they should be careful that this does not lead to unreasonable restrictions on pupils’ ability to assess and manage risks themselves.

Consider if there is any potential liability in a situation that a monitoring alert is received out of school hours. For example, in a situation that an alert is received during the night that a pupil had accessed a website with harmful content. Although this information would be readily available to school from the time the alert was received it would likely not be reviewed for some hours.

It is important that schools are clear with parents when monitoring of devices will take place and how alerts of this nature, received ‘out of hours,’ will be dealt with. If schools opt to offer 24/7 monitoring, it must be clearly communicated to parents that the school would not be held liable for a pupil’s actions if any monitoring alerts are not reviewed straightaway.

Filtering and monitoring continued

141. …governing bodies and proprietors should be doing all that they reasonably can to **limit children's exposure to the four risks** *from the school's or college's IT system….governing bodies and proprietors should ensure their school or college has* **appropriate filtering and monitoring systems in place and regularly review their effectiveness… leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns** *when identified. Governing bodies and proprietors should consider the* **number of** *and* **age range of their children, those who are potentially at greater risk of harm** *and* **how often they access the IT system** *along with the* **proportionality of costs versus safeguarding risks**

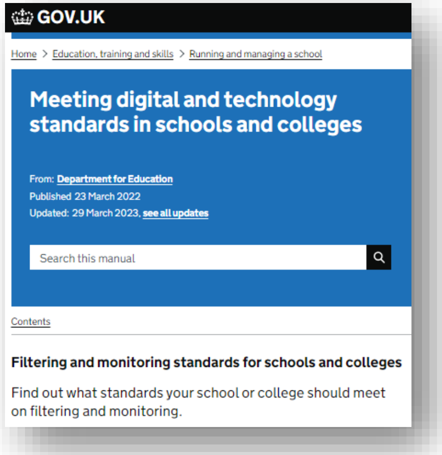
- How knowledgeable are your governors about the filtering and monitoring systems in place?
- Are governors involved in reviewing monitoring and filtering provisions as part of safeguarding responsibilities?

DfE Meeting digital and technology standards in schools and colleges

Filtering and monitoring standards in schools and colleges

2. Review provision at least annually

2. Review your filtering and monitoring provision at least annually



GOV.UK

Home > Education, training and skills > Running and managing a school

Meeting digital and technology standards in schools and colleges

From: Department for Education
Published 23 March 2022
Updated: 29 March 2023, see all updates

Contents

Filtering and monitoring standards for schools and colleges

Find out what standards your school or college should meet on filtering and monitoring.

Checks should include a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

Checks should be recorded:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

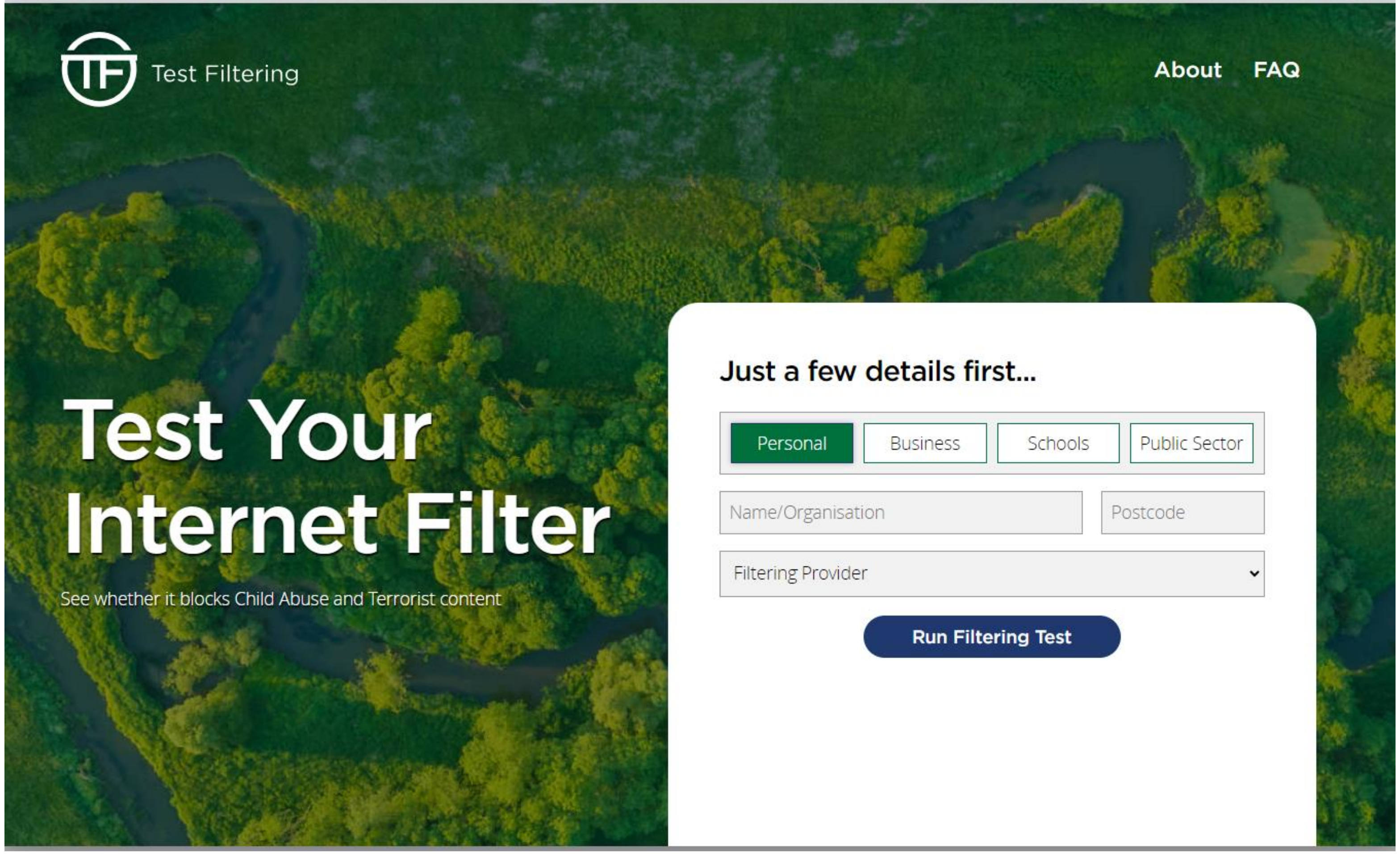
The review should be conducted by the responsible governor, a member of the senior leadership team, the DSL, and the IT service provider (if appropriate)

Securus and device types

Windows devices require the **client software** to be **installed**

Chromebook devices require a **Google extension** to be **installed**

iPad require a **proxy** to be created and **proxy settings** to be applied for the internet traffic that is passing through the web browser (Safari) to be monitored



Test Filtering

About FAQ

Test Your Internet Filter

See whether it blocks Child Abuse and Terrorist content

Just a few details first...

http://testfiltering.com/

Understanding your risk profile

Risk Vs Harm

What are your filtering and monitoring systems trying to mitigate against?

CONTENT

CONTACT

CONDUCT

COMMERCE

When assessing your risk, consider:

- age of learners
- ability of learners
- vulnerabilities of learners
- type of device being used by learners
- activities learners are expected to do
- are devices taken home for use?
- staff confidence with technology

- support available to staff
- trends of incidences in the past
- what is being taught as regards online safety
- what support is offered to parents? how knowledgeable are parents to support, enforce, identify and report?
- is there an open, trusted culture with a willingness to report?

Are your filtering and monitoring systems mitigating against your risks? Are they working to support your organisations risk profile?

Checking, documenting and evidencing

Policies and procedures should be robust and fit for purpose with filtering and monitoring in mind

138. *Online safety and the school or college's approach to it should be reflected in the* **child protection policy** *which, amongst other things,* **should include appropriate filtering and monitoring on school devices and school networks**.

Department for Education

Behaviour in schools

Advice for headteachers and school staff

September 2022

Monitoring and evaluating school behaviour section

Guidance on specific behaviour issues section:

- child-on-child sexual violence and sexual harassment
- behaviour incidents online
- suspected criminal behaviour

Checking, documenting and evidencing

- Have any recent safeguarding reports been flagged by filtering and monitoring?
- Incidents should be recorded through safeguarding processes
- What the systems should and are blocking and allowing - the reviews of filtering and monitoring should inform your future strategy and actions
- Action planning should be documented and progress on identified areas of risk should be evaluated
- Have ‘at risk’ individuals been identified and are proactively monitored?

142. The **appropriateness of any filtering and monitoring systems** are a matter for individual schools and colleges and will be **informed in part, by the risk assessment required by the Prevent Duty**.

- Useful to carry out and evidence ‘What if..?’ scenarios to inform checks to be conducted

Examples of ‘What if…?’ scenarios

1. What if a user was to use an incognito/private browser to search for inappropriate content. Would our systems report this?

2. What if users have a generic log in. How can we identify who did it?

3. What if a user is sent inappropriate content rather than creating it. Would our systems pick this up?

4. What if the filtering requests are not closely managed and the filter is not reapplied after the time approved?

5. What if a school owned device is taken home. Will filtering and monitoring still work?

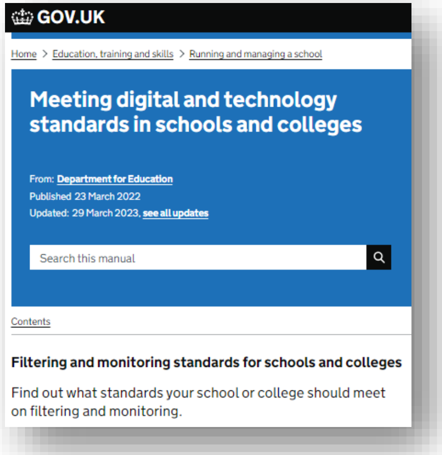
6. What if a user logs in with someone else's log in credentials and accesses inappropriate content. What are the consequences of this? Is it reflected in policies for behaviour?

DfE Meeting digital and technology standards in schools and colleges

Filtering and monitoring standards in schools and colleges

3. Block harmful and inappropriate content

3. Filtering systems should block harmful and inappropriate content, without unreasonably impacting teaching and learning



GOV.UK

Home > Education, training and skills > Running and managing a school

Meeting digital and technology standards in schools and colleges

From: Department for Education
Published 23 March 2022
Updated: 29 March 2023, see all updates

Filtering and monitoring standards for schools and colleges

Find out what standards your school or college should meet on filtering and monitoring.

- filter all internet feeds, including any backup connections
- be age and ability appropriate for the users, and be suitable for educational settings
- handle multilingual web content, images, common misspellings and abbreviations
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide alerts when any web content has been blocked

134. Whilst it is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place, they should be **careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding***.*

What have you decided to block access to?

Do you allow access to YouTube?

If you are blocking it what is your reason for this?

Ofcom research shows that YouTube is the most popular service used by children and young people

Does blocking YouTube lead to “over blocking” and therefore leads to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding?

Filtering providers must be:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

Filtering systems *should*:

be operational, up to date and applied to all:

- users, including guest accounts
- school owned devices
- devices using the school broadband connection

allow you to identify:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

Staff responsibility regarding filtering systems

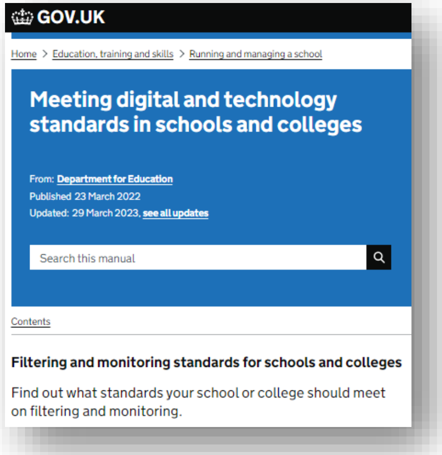
- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

DfE Meeting digital and technology standards in schools and colleges

Filtering and monitoring standards in schools and colleges

4. Effective monitoring strategies

4. Effective monitoring strategies that meet the safeguarding needs of your school or college



GOV.UK

Home > Education, training and skills > Running and managing a school

Meeting digital and technology standards in schools and colleges

From: Department for Education
Published 23 March 2022
Updated: 29 March 2023, see all updates

Search this manual

Contents

Filtering and monitoring standards for schools and colleges

Find out what standards your school or college should meet on filtering and monitoring.

A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

To meet standard 4:

DSL takes lead responsibility for any safeguarding and child protection matters that are picked up through monitoring

Management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective

Review of effectiveness of monitoring and reporting processes is done by SLT and supported by governing body

Training should be provided to make sure knowledge is current. You may need to ask your monitoring system provider for system specific training and support

Review of effectiveness should include

- How well incidents are urgently picked up, acted on and outcomes recorded
- Check of staff understanding as to how to deal with incidents of a malicious, technical, or safeguarding nature and who should lead on any actions
- Monitoring data is received in a format that staff can understand
- Users are identifiable so concerns can be traced back to an individual, including guest accounts
- Ensuring mobile or app technologies have a technical monitoring system applied to the devices
- Review of AUP, online safety, safeguarding and organisational policies such as privacy notice to include your organisations monitoring procedures
- If your organisation is using a technical monitoring system then you must have a DPIA which should be reviewed along with privacy notices of third-party providers to check all details are relevant, accurate and as required